Institution		**Date of Exam**	
Charter		**Prepared By**	

#11 - INFORMATION TECHNOLOGY SNAPSHOT WORKPROGRAM

PART 1 – RISK ASSESSMENT

An IT risk assessment is a multi-step process of identifying and quantifying threats to information assets in an effort to determine cost effective risk management solutions. To help us assess your risk management practices and the actions taken as a result of your risk assessment, please answer the following questions.

YES	NO	
		a. Name and title of individual(s) responsible for managing the IT risk assessment process [*FDIC Rules and Regulations, Part 364, Appendix B, Section III (A)(2)]*:
		b. Names and titles of individuals, committees, departments or others participating in the risk assessment process. If third-party assistance was utilized during this process, please provide the name and address of the firm providing the assistance and a brief description of the services provided *[FDIC Rules and Regulations, Part 364, Appendix B, Section III (A)(2)]*:
		c. Does your written information security program include a risk assessment *[FDIC Rules and Regulations, Part 364, Appendix B, Section III (B)]*?
		d. Does the scope of your risk assessment include an enterprise-wide analysis of internal and external threats and vulnerabilities to confidential customer and consumer information; the likelihood and impact of identified threats and vulnerabilities; and the sufficiency of policies, procedures, and customer information systems to control risks *[FDIC Rules and Regulations, Part 364, Appendix B, Section III(B)]*?
		e. Do you have procedures for maintaining asset inventories and identifying customer information at the institution, in transit, and at service providers *[FDIC Rules and Regulations, Part 364, Appendix B, Section III (B); FFIEC IT Examination Handbook, Information Security Booklet]*?
		f. Do risk assessment findings clearly identify the assets requiring risk reduction strategies *[FDIC Rules and Regulations, Part 364, Appendix B, Section III (B); FFIEC IT Examination Handbook, Information Security Booklet]*?
		g. Do written information security policies and procedures reflect risk reduction strategies for the assets identified in "f" above *[FDIC Rules and Regulations, Part 364, Appendix B, Section III (C)(1); FFIEC IT Examination Handbook, Information Security Booklet]*?
		h. Were changes in technology (e.g., service provider relationships, software applications, and/or service offerings) implemented since the previous examination reflected in your risk assessment *[FDIC Rules and Regulations, Part 364, Appendix B, Section III (C) and (E); FFIEC IT Examination Handbook, Information Security Booklet]*?
		If "No," which technology changes were excluded?
		i. Is your risk assessment *program* formally approved by the Board of Directors at least annually *[FDIC Rules and Regulations, Part 364, Appendix B, Section III (A)(1) and (F)]*?
		If yes, please provide the date that the risk assessment program was last approved by the Board of Directors:
		j. Has a report of risk assessment *findings* been presented to the Board of Directors for review and acceptance *[FDIC Rules and Regulations, Part 364, Appendix B, Section III (F)]*?
		If yes, please provide the date that the risk assessment findings were last approved by the

YES	NO	
		Board of Directors:
		k. Are you planning to deploy new technology within the next 12 months?
		If "Yes," were the risks associated with this new technology reviewed during your most recent risk assessment *[FDIC Rules and Regulations, Part 364, Appendix B, Section III (E); FFIEC IT Examination Handbook, Information Security Booklet]*?

1. Evaluate and comment upon whether the risk management process provides a comprehensive program to identify and monitor risk relative to size, complexity, and risk profile of the entity.

Examiner Comments:

2. Evaluate and comment upon whether management and the Board have demonstrated the ability to successfully address existing IT problems and potential risks, including prompt resolution of audit and regulatory concerns.

Examiner Comments:

If needed, provide additional comments regarding the bank's risk assessment function.

Additional Comments:

Institution		**Date of Exam**	
Charter		**Prepared By**	

11- INFORMATION TECHNOLOGY SNAPSHOT WORKPROGRAM

PART 2 – OPERATIONS SECURITY AND RISK MANAGEMENT

To help us assess how you manage risk through your information security program, please answer the following questions for your environment. If any of the following questions are not applicable to your environment, simply answer "N/A."

YES	NO	
		a. Do you have a written information security program designed to manage and control risk *[FDIC Rules and Regulations, Part 364, Appendix B, Section II (A) and Section III (C)(1)]*?
		If "Yes," please provide the date that the written information security program was last approved by the Board of Directors *[FDIC Rules and Regulations, Part 364, Appendix B, Section III (A)(1)]*:
		b. Does your information security program contain written policies, procedures, and guidelines for securing, maintaining, and monitoring the following systems or platforms [*FFIEC IT Examination Handbook, Information Security Booklet; FIL-12-1999, Uniform Rating System for Information Technology]*:
		1. Core banking system?
		2. Imaging?
		3. Remote deposit capture?
		4. Payment systems (including wire transfer and ACH)?
		5. Voice over IP telephony?
		6. Instant messaging?
		7. Virtual private networking?
		8. Wireless networking – LAN or WAN?
		9. Local area networking?
		10. Wide area networking?
		11. Routers?
		12. Modems or modem pools?
		13. Security devices such as firewall(s) and proxy devices?
		14. Other remote access connectivity such as GoToMyPC, PcAnyWhere, etc.?
		15. Portable devices such as PDAs, laptops, cell phones, etc.?
		16. Hard drive or flash memory of photocopiers, fax machines and printers erased, encrypted or destroyed prior to being returned to the leasing company, sold to a third party or otherwise disposed of? *(FIL-56-2010)*
		17. Other – please list:
		c. Do you employ access controls on customer information systems *[FDIC Rules and Regulations, Part 364, Appendix B, Section III (C)(1)(a); FFIEC IT Examination Handbook, Information Security Booklet; FIL-103-2005, Authentication in an Internet Banking Environment]*?
		d. Do you have a physical security program which defines and restricts access to information assets as well as protects against destruction, loss, or damage of customer information *[FDIC Rules and Regulations, Part 364, Appendix B, Section III (C)(1)(b) and (h); FFIEC IT Examination Handbook, Information Security Booklet]*?

YES	NO	
		e. Do you encrypt customer information *[FDIC Rules and Regulations, Part 364, Appendix B, Section III (C)(1)(c); FFIEC IT Examination Handbook, Information Security Booklet]*?
		If "Yes," describe where encryption has been implemented:
		f. Do you have formal configuration, change management, and patch management procedures for all applicable platforms identified in "b" above *[FDIC Rules and Regulations, Part 364, Appendix B, Section III (C)(1)(d); FFIEC IT Examination Handbook, Information Security Booklet; FIL-43-2003, Guidance on Developing an Effective Software Patch Management Program]*?
		g. Does your information security program incorporate dual control procedures, segregation of duties, and employee background checks for employees with responsibilities for, or access to, customer information *[FDIC Rules and Regulations, Part 364, Appendix B, Section III (C)(1)(e)]*?
		h. Do you have formal logging/monitoring requirements for platforms identified in "b" above *[FDIC Rules and Regulations, Part 364, Appendix B, Section III (C)(1)(f); FFIEC IT Examination Handbook, Information Security Booklet]*?
		i. Do you have a formal intrusion detection program, other than basic logging, for monitoring host and/or network activity *[FDIC Rules and Regulations, Part 364, Appendix B, Section III (C)(1)(f); FFIEC IT Examination Handbook, Information Security Booklet]*?
		j. Do you have an incident response plan defining responsibilities and duties for containing damage and minimizing risks to the institution and customers *[FDIC Rules and Regulations, Part 364, Appendix B, Section III (C)(1)(g); FFIEC IT Examination Handbook, Information Security Booklet]*?
		If "Yes," does the plan include customer notification procedures *[FDIC Rules and Regulations, Part 364, Appendix B, Supplement A; FIL-27-2005, Response Programs for Unauthorized Access to Customer Information and Customer Notice]*?
		k. Please provide the names and titles and/or committee members charged with formally overseeing and implementing the information security program *[FDIC Rules and Regulations, Part 364, Appendix B, Section II (A) and Section III (A)(2)]*:
		l. Do you maintain topologies, diagrams, or schematics depicting your physical and logical operating environment(s) *[FDIC Rules and Regulations, Part 364, Appendix B, Section III (B); FFIEC IT Examination Handbook, Information Security Booklet]*?
		m. Do you have a process in place to monitor and adjust, as appropriate, the information security program *[FDIC Rules and Regulations, Part 364, Appendix B, Section III (E)]*?
		n. Do you have an employee acceptable use policy *[FDIC Rules and Regulations, Part 364, Appendix B, Section III (C)(2); FFIEC IT Examination Handbook, Information Security Booklet]*?
		If "Yes," please provide how often employees must attest to the policy contents:
		o. Do you have an employee security awareness training program *[FDIC Rules and Regulations, Part 364, Appendix B, Section III (C)(2); FFIEC IT Examination Handbook, Information Security Booklet]*?
		If "Yes," please indicate the last date training was provided:
		p. Does the institution report the overall status of the information security program and compliance with the Interagency Guidelines Establishing Information Security Standards to the Board or designated committee *[FDIC Rules and Regulations, Part 364, Appendix B, Section III (F)]*?
		If "Yes", please provide the date that the findings were most recently approved by the Board of Directors:
		q. Does the institution's strategic planning process incorporate information security *[FFIEC IT Examination Handbook, Management Booklet]*?

YES	NO	
		r. Do you have policies/procedures for the proper disposal of customer and consumer information *[FDIC Rules and Regulations, Part 364, Appendix B, Section III (C)(4); FIL-7-2005, Fair and Accurate Credit Transactions Act of 2003, Guidelines Requiring the Proper Disposal of Consumer Information]*?
		s. Is a formal process in place to address changes to, or new issuance of, laws/regulations and regulatory guidelines *[FDIC Rules and Regulations, Part 364, Appendix B, Section III (E); FFIEC IT Examination Handbook, Management Booklet]*?
		t. Have you experienced any material security incidents (internal or external) affecting the institution or institution customers since the prior IT examination *[FDIC Rules and Regulations, Part 364, Appendix B, Section III (C)(1)(g); FIL-27-2005, Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice]*?
		u. Do you serve as an Originating Depository Financial Institution (ODFI)?
		If "Yes," do ACH policies/procedures address individual responsibilities, separation of duties, funds availability/credit limits, third-party agreements, information security, business continuity plans, insurance protections, and vendor management *[FFIEC IT Examination Handbook, Retail Payment Systems Booklet]*?
		v. If you serve as an ODFI, do all originators have direct agreements with your institution?
		If "No," are written agreements in place with third-party senders and/or third party service providers that address originator underwriting and liabilities *[FFIEC IT Examination Handbook, Retail Payment Systems Booklet; NACHA Rule Book]*?
		w. Do wire transfer policies/procedures address responsibilities and authorizations, separation of duties, funds availability/credit limits, information security, business continuity plans, insurance protections, and vendor management *[FFIEC IT Examination Handbook, Retail Payment Systems Booklet]*?
		x. Do you serve as a merchant acquirer for credit card activity?
		If "Yes," do you have written policies/procedures that address merchant approval/termination, underwriting, fraud and credit monitoring, chargeback processing and control, and agent bank programs?
		y. Are project management techniques and system development life cycle processes used to guide efforts at acquiring and implementing technology *[FFIEC IT Examination Handbook, Development and Acquisition Booklet; FIL-12-1999, Uniform Rating System for Information Technology]*?

1. Evaluate and comment upon the degree to which the organization provides technology services that are reliable and consistent.

Examiner Comments:

2. Evaluate and comment upon whether written technology plans, policies, procedures, and standards are thorough and properly reflect the complexity of the IT environment. Also, evaluate and comment upon whether these plans, policies, procedures and standards have been formally adopted, communicated, and enforced throughout the organization, including a formal written data security policy and awareness program.

Examiner Comments:

3. Evaluate and comment upon whether logical and physical security for all IT platforms is closely monitored, and whether security incidents and weaknesses are identified and quickly corrected.

Examiner Comments:

4. Evaluate and comment upon the degree to which IT operations are reliable, and risk exposure is successfully identified and controlled. Include in this evaluation criteria an assessment of management's risk mitigation in the payment systems area (including wire transfer and ACH activities).

Examiner Comments:

5. Evaluate and comment upon the degree to which IT strategic plans are well-defined and fully integrated throughout the organization.

Examiner Comments:

6. Evaluate and comment on whether management and the Board routinely demonstrate the ability to identify and implement appropriate IT solutions while effectively managing risk.

Examiner Comments:

7. Evaluate and comment upon whether project management techniques and the Systems Development Life Cycle (SDLC) are fully effective and supported by written policies, procedures, and project controls that consistently result in timely and efficient project completion.

Examiner Comments:

8. Evaluate and comment upon the degree to which an independent quality assurance function provides strong controls over testing and program change management.

Examiner Comments:

9. Evaluate and comment upon whether technology solutions consistently meet end-user needs.

Examiner Comments:

10. Banks should be aware of the risks posed by the potential disclosure of sensitive customer information stored on the hard drive or flash memory of photocopiers, fax machines and printers used by the institution. Determine if the bank has written policies and procedures to identify devices that store digital images of business documents and ensure their hard drive or flash memory is erased, encrypted or destroyed prior to being returned to the leasing company, sold to a third party or otherwise disposed of. (Per FIL 56-2010)

FIL 56-2010

Examiner Comments:

If needed, provide additional comments regarding the bank's operation security and risk management function.

Additional Comments:

Institution		**Date of Exam**	
Charter		**Prepared By**	

#11 - INFORMATION TECHNOLOGY SNAPSHOT WORKPROGRAM

PART 3 – AUDIT/INDEPENDENT REVIEW PROGRAM

To help us assess how you monitor operations and compliance with your written information security program, please answer the following questions.

YES	NO	
		a. Please provide the name and title of the IT auditor or employee performing the internal IT audit function. Include who this person reports to and a brief description of their education and experience conducting IT audits *[FDIC Rules and Regulations, Part 364, Appendix A, Section II (B), and Appendix B, Section III (C)(3); FFIEC IT Examination Handbook, Audit Booklet]*:
		b. Do you have a written IT audit/independent review program that is based on the results of a risk analysis *[FDIC Rules and Regulations, Part 364, Appendix B, Section III (C)(3); FFIEC IT Examination Handbook, Audit Booklet]*?
		c. Please provide the following information regarding your most recent IT audit/independent reviews *[FDIC Rules and Regulations, Part 364, Appendix B, Section III (C)(3) and (F); FFIEC IT Examination Handbook, Audit Booklet; FIL-12-1999 Uniform Rating System for Information Technology]*:

	Audit Date	Entity Conducting Audit	Written Audit Report (Y/N)	Audit Committee/ Board Review Date
Information Security Program				
IT General Controls Review				
Vulnerability Testing				
Penetration Testing				
Wire Transfer Audit				
NACHA Rule Compliance Audit				
Other:				
Other:				

YES	NO	
		d. Does audit coverage include a comparison of actual system configurations to documented/baseline configuration standards *[FDIC Rules and Regulations, Part 364, Appendix B, Section III (C)(3); FFIEC IT Examination Handbook, Information Security Booklet]*?
		e. Does audit coverage include assessing compliance with the information security program requirements *[FDIC Rules and Regulations, Part 364, Appendix B, Section III (C)(3); FFIEC IT Examination Handbook, Information Security Booklet]*?
		f. Does audit coverage include assessing users and system services access rights *[FDIC Rules and Regulations, Part 364, Appendix B, Section III (C)(3); FFIEC IT Examination Handbook, Information Security Booklet]*?

YES	NO	
		g. Are the results of your audits/independent reviews used to adjust your risk assessment findings/results *[FDIC Rules and Regulations, Part 364, Appendix B, Section III (C)(3) and (E); FFIEC IT Examination Handbook, Information Security Booklet]*?
		h. Briefly describe any known conflicts or concentrations of duties *[FDIC Rules and Regulations, Part 364, Appendix A, Section II (B), and Appendix B, Section III (C)(1)(e) and (3); FFIEC IT Examination Handbook, Audit Booklet]*:
		i. Do you have a system for tracking audit and regulatory exceptions to final resolution *[FDIC Rules and Regulations, Part 364, Appendix B, Section III (C)(3) and (E); FFIEC IT Examination Handbook, Audit Booklet]*?

1. Evaluate and comment upon the degree to which the risk analysis process ensures that audit plans address all significant IT operations, procurement, and development activities with appropriate scope and frequency.

Examiner Comments:

2. Evaluate and comment upon the degree to which the audit function is independent and identifies and reports weaknesses and risks to the Board of Directors or its audit committee in a thorough and timely manner.

Examiner Comments:

3. Evaluate and comment upon whether outstanding audit issues are monitored until resolved.

Examiner Comments:

4. Evaluate and comment upon whether audit work is performed in accordance with professional auditing standards and report content is timely, constructive, accurate, and complete.

Examiner Comments:

5. Evaluate and comment upon the degree to which the board of directors and examiners can rely on the audit results.

Examiner Comments:

If needed, provide additional comments regarding the bank's audit and independent review function.

Additional Comments:

Institution		**Date of Exam**	
Charter		**Prepared By**	

#11 - INFORMATION TECHNOLOGY SNAPSHOT WORKPROGRAM

PART 4 - DISASTER RECOVERY AND BUSINESS CONTINUITY

To help us assess your preparedness for responding to and recovering from an unexpected event, please answer the following.

YES	NO	
		a. Do you have an organization-wide disaster recovery and business continuity program *[FDIC Rules and Regulations, Part 364, Appendix B, Section III (C)(1)(h); FFIEC IT Examination Handbook, Business Continuity Planning Booklet]*?
		If yes, please provide the name of your coordinator:
		b. Does your business continuity program include influenza pandemic preparedness guidelines *[FIL-25-2006, Influenza Pandemic Preparedness Interagency Advisory]*?
		c. Are disaster recovery and business continuity plans based upon a business impact analysis *[FDIC Rules and Regulations, Part 364, Appendix B, Section III (C)(1)(h); FFIEC IT Examination Handbook, Business Continuity Planning Booklet]*?
		If "Yes," do the plans identify recovery and processing priorities?
		d. Do you have formal agreements for an alternate processing site and equipment should the need arise to relocate operations *[FDIC Rules and Regulations, Part 364, Appendix B, Section III (C)(1)(h); FFIEC IT Examination Handbook, Business Continuity Planning Booklet]*?
		e. Do business continuity plans address procedures and priorities for returning to permanent and normal operations *[FDIC Rules and Regulations, Part 364, Appendix B, Section III (C)(1)(h); FFIEC IT Examination Handbook, Business Continuity Planning Booklet]*?
		f. Do you maintain offsite backups of critical information *[FDIC Rules and Regulations, Part 364, Appendix B, Section III (C)(1)(h); FFIEC IT Examination Handbook, Business Continuity Planning Booklet]*?
		If "Yes," is the process formally documented and audited?
		g. Do you have procedures for testing backup media at an offsite location *[FDIC Rules and Regulations, Part 364, Appendix B, Section III (C)(1)(h); FFIEC IT Examination Handbook, Business Continuity Planning Booklet]*?
		h. Have disaster recovery/business continuity plans been tested *[FDIC Rules and Regulations, Part 364, Appendix B, Section III (C)(1)(h); FFIEC IT Examination Handbook, Business Continuity Planning Booklet]*?
		If "Yes", please identify the system(s) tested, the corresponding test date, and the date reported to the Board:

1. Evaluate and comment upon whether management has a comprehensive corporate contingency and business resumption program in place.

Examiner Comments:

2. Evaluate and comment upon whether annual contingency plan testing and updating is adequate, and whether test results evidence that critical systems and applications are recovered within acceptable time frames.

Examiner Comments:

If needed, provide additional comments regarding the bank's disaster recovery and business continuity management function.

Additional Comments:

Institution		**Date of Exam**	
Charter		**Prepared By**	

#11 - INFORMATION TECHNOLOGY SNAPSHOT WORKPROGRAM

PART 5 – Vendor Management and Service Provider Oversight

Given the increased reliance on outside firms for technology-related products and services, please answer the following questions to help us assess the effectiveness of your vendor management and service provider oversight programs.

YES	NO	
		a. Does your vendor management program address due diligence, contract provision, financial condition, risk assessment, ongoing monitoring requirements, and third-party relationships such as subcontractors and agents *[FDIC Rules and Regulations, Part 364, Appendix B, Section III (D); FIL-812000, Risk Management of Technology Outsourcing]*?
N/A		b. Has the bank identified and reported its service provider relationships (both domestic and foreign-based) to the FDIC *["Notification of Performance of Bank Services," FDIC Rules and Regulations, 304.3 and 12USC1867, Section 7(c)(2), Bank Service Company Act (BSCA)]*? **Unless the FDIC verifies that this has been done, mark as N/A.**
		c. Are all of your direct or indirect service providers located within the United States?
		If "No," has management provided risk management policies; performance monitoring and oversight processes; legal and technical expertise; and access to critical, material, or sensitive customer information to address unique risks from these outsourcing relationships *[FIL-52-2006, Foreign-Based Third-Party Service Providers Guidance on Managing Risks in These Outsourcing Relationships]*?
		d. Do licensing agreements for core processing or mission-critical applications require vendors to maintain application software so that the software operates in compliance with all applicable federal and state regulations *[FIL-121-2004, Computer Software Due Diligence Guidance on Developing an Effective computer Software Evaluation Program to Assure Quality and Regulatory Compliance]*?
		e. Do you require your service providers by contract to implement measures designed to meet the objectives of the Interagency Guidelines Establishing Information Security Standards *[FDIC Rules and Regulations, Part 364, Appendix B, Section III (D)(2)]*?
		f. Where indicated by the risk assessment, do you review audits, summaries of test results, and other equivalent evaluations of your service providers to confirm that they are fulfilling contractual obligations to implement appropriate measures designed to meet the objectives of the Interagency Guidelines Establishing Information Security Standards *[FDIC Rules and Regulations, Part 364, Appendix B, Section III (D)(3)*?

1. Evaluate and comment upon the degree to which outsourcing arrangements are based on comprehensive planning, and whether routine management supervision sustains an appropriate level of control over vendor contracts, performance, and services provided.

Examiner Comments:

If needed, provide additional comments regarding the bank's vendor management program.

Additional Comments:

Institution		**Date of Exam**	
Charter		**Prepared By**	

#11 - INFORMATION TECHNOLOGY SNAPSHOT WORKPROGRAM

PART 6 – INTERAGENCY GUIDELINES ESTABLISHING INFORMATION SECURITY STANDARDS

Evaluate if the bank's information security program adequately meets the objectives of safeguarding customer information guidelines and subsequent interpretive guidance.

- Ensures the security and confidentiality of customer information;
- Protects against any anticipated threats or hazards to the security or integrity of such information;
- Protects against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer;
- Ensures the proper disposal of customer information and consumer information.
- Implements appropriate authentication in an Internet banking environment; and
- Ensures appropriate response programs for unauthorized access.

Examiner Comments:

Complete the Summary of Findings for the full IT RMP.

Institution		**Date of Exam**	
Charter		**Prepared By**	

SUMMARY OF FINDINGS

#11 – IT RMP

Describe all strengths evident from the evaluation.

Describe all weaknesses evident from evaluation, including violations of law/regulation/rules; noncompliance with Departmental policies/guidelines; internal policy deficiencies/ noncompliance; internal control weaknesses; MIS problems; and deficiencies in management supervision.

Report Worthy:

Not Report Worthy:

Determine why weaknesses exist and comment on management's response and plan of action. Identify bank personnel making the response.

SUMMARY RISK RATING ASSIGNED: ☐

Definitions:

1-Strong; 2-Satisfactory; 3-Less than satisfactory; 4-Deficient; 5-Critically deficient; NR-Not Rated

(Return to Core Analysis)

Provide copy of this page to EIC/AEIC. Receipt and review of this form by the EIC/AEIC will be evidenced bsy his/her initials in the appropriate column for this procedure on the SCOPE AND REVIEW ACKNOWLEDGEMENT FORM (Planning and Control Worksheet #1).